Amendments to the Claims

An amended Listing of Claims are on pages 4–10.

Claims 93, 95, and 103 have been canceled.

Claims 90, 91, 100, and 104 are currently amended.

There are no new claims.

Claims 90–92, 94, 96–102, and 104–108 are pending.

Listing of Claims:

Claims 1-89 (Canceled)

90. (Currently amended) A method of securely distributing program instructions for execution in a single-chip secure cryptoprocessor that contains ~~substantially unique~~ chip identifier data that distinguishes different cryptoprocessor units, encryption circuitry for encrypting said identifier, decryption circuitry for decrypting encrypted digital program instructions, writable program memory for storing decrypted instructions, and processor core for executing said decrypted instructions which are inaccessible from said secure cryptoprocessor chip from locations outside of said chip after fabrication of said chip is completed; the method comprising:

(a) encrypting in a network server a first program of executable digital instructions under control of a first encryption key;

(b) transmitting said encrypted first program of digital instructions from said server to said cryptoprocessor;

(c) encrypting said ~~unique~~ chip identifier in said cryptoprocessor chip to produce an encrypted identifier;

(d) transmitting said encrypted identifier to said server;

(e) reencrypting in said server said ~~unique~~ chip identifier together with a decryption key corresponding to said first encryption key to produce at least one encrypted data block such that each bit in said encrypted data block is a complex function of every bit in said decryption key and every bit in said chip identifier;

(f) transmitting said data block to said cryptoprocessor chip;

(g) decrypting said encrypted data block in said cryptoprocessor chip to produce a decrypted identifier and said decryption key in said cryptoprocessor chip;

(h) decrypting said encrypted first program in said cryptoprocessor chip under control of said decryption key to produce executable digital instructions stored in said program memory; and

(i) executing said digital instructions in said processor core in said cryptoprocessor chip to generate output data if said decrypted identifier has a predetermined relationship with said ~~unique~~ chip identifier in said cryptoprocessor chip.

91. (Currently amended) The method of claim 90, further comprising the steps of

(j) generating a session key in said server;

(k) transmitting said session key in encrypted form to said cryptoprocessor;

(l) decrypting said encrypted session key in said cryptoprocessor chip to produce a decrypted session key;

(m) encrypting said ~~unique~~ chip identifier in said cryptoprocessor chip under control of said decrypted session key to produce said encrypted identifier; and

(n) decrypting said encrypted identifier in said server under control of said session key to produce a decrypted identifier.

92. (Previously presented) The method of claim 90, wherein said cryptoprocessor chip is a component in a video game system and said output data generated by said cryptoprocessor is game data that is processed by a graphics co-processor in said game system that generates graphics data for display on a display device.

93. (Canceled)

94. (Previously presented) The method of claim 90, wherein said cryptoprocessor chip is a component in a computer and said output data generated by said cryptoprocessor is address data that identifies memory locations of non-encrypted program instructions executed by a second processor in said computer.

95. (Canceled)

96. (Previously presented) The method of claim 90, wherein said cryptoprocessor chip communicates with a second processor through a data transmission path that comprises wireless transmission.

97. (Previously presented) The method of claim 90, wherein said cryptoprocessor chip inhibits output of said executable digital instructions from said data memory to a location outside of said secure cryptoprocessor chip.

98. (Previously presented) The method of claim 90, wherein said output data generated by said cryptoprocessor contain instructions that are executed by a second processor.

99. (Previously presented) The method of claim 90, further comprising the step of downloading said encrypted first program of executable digital instructions and said encrypted data block through a retailer computer.

100. (Currently amended) A computer readable data storage medium having stored thereon encrypted digital program instructions for execution in a single-chip secure cryptoprocessor that contains ~~substantially unique~~ chip identifier data that distinguishes different cryptoprocessor units, encryption circuitry for encrypting said identifier, decryption circuitry for decrypting encrypted digital program instructions, writable program memory for storing decrypted instructions, and processor core for executing said decrypted instructions which are inaccessible from said secure cryptoprocessor chip from locations outside of said chip after fabrication of said chip is completed, wherein said cryptoprocessor chip performs the following:

(a) encrypting said ~~unique~~ chip identifier in said cryptoprocessor chip to produce an encrypted identifier for transmission to a network server that encrypts and downloads a first program of executable digital instructions for use in said cryptoprocessor, wherein said server decrypts said encrypted identifier to produce a decrypted identifier, and wherein said server reencrypts said decrypted identifier together with a decryption key corresponding to said encrypted first program to produce at least one encrypted data block for transmission to said cryptoprocessor chip such that each bit in said encrypted data block is a complex function of every bit in said decryption key and every bit in said chip identifier;

(b) decrypting said encrypted data block in said cryptoprocessor chip to produce a decryption key in said cryptoprocessor chip;

(c) decrypting said encrypted first program in said cryptoprocessor chip under control of said decryption key to produce executable digital instructions stored in said program memory; and

(d) executing said digital instructions in said processor core in said cryptoprocessor chip to generate output data if said decrypted identifier has a predetermined relationship with said ~~unique~~ chip identifier in said cryptoprocessor chip.

101. (Previously presented) The data storage medium of claim 100, further storing nonencrypted digital program instructions for execution in a second processor that processes said output data from said cryptoprocessor chip and generates second data that is processed by said cryptoprocessor chip.

102. (Previously presented) The data storage medium of claim 100, further storing said encrypted data block in said data storage medium.

103. (Canceled)

104. (Currently amended) A single-chip secure cryptoprocessor comprising:

(a) non-volatile data memory storing ~~substantially unique~~ chip identifier data that distinguishes different cryptoprocessor chips;

(b) encryption circuitry for encrypting said ~~unique~~ chip identifier to produce an encrypted identifier for transmission to a network server;

(c) wherein said server encrypts and downloads a first program of executable digital instructions for use in said cryptoprocessor, wherein said server decrypts said encrypted identifier to produce a decrypted identifier, and wherein said server reencrypts said decrypted identifier together with a digital decryption key corresponding to said encrypted first program to produce at least one encrypted data block for use in said cryptoprocessor chip such that each bit in said encrypted data block is a complex function of every bit in said decryption key and every bit in said chip identifier;

(d) decryption circuitry for decrypting said encrypted data block to produce a decrypted key;

(e) writable data memory for storing said decrypted key;

(f) decryption circuitry for decrypting said first program under control of said decrypted key to produce executable digital decrypted instructions;

(g) writable program memory for storing said decrypted instructions; ~~and~~

(h) processor core for executing said decrypted instructions to produce output data if said decrypted identifier has a predetermined relationship with said ~~unique~~ chip identifier; and

(i) wherein said data memory, encryption circuitry, decryption circuitry, processor core, program memory, and decrypted instructions are inaccessible from said secure cryptoprocessor chip from locations outside of said secure cryptoprocessor chip after fabrication of said chip is completed.

105. (Previously presented) The cryptoprocessor chip of claim 104, wherein said cryptoprocessor chip communicates with a second processor through a data transmission link that comprises wireless transmission.

106. (Previously presented) The cryptoprocessor chip of claim 104, wherein said output data is processed by a second processor in one of the group comprising: a video game system, a handheld game system, and a computer.

107. (Previously presented) The cryptoprocessor chip of claim 104, wherein said cryptoprocessor chip is a component in one of the group comprising: a video game system, a handheld game system, and a computer.

108. (Previously presented) The cryptoprocessor chip of claim 104, wherein said writable program memory is non-volatile.